IN THE UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF PENNSYLVANIA
PITTSBURGH DIVISION

HERITAGE VALLEY HEALTH SYSTEM, INC., a Pennsylvania non-profit corporation,	)	
Plaintiff,	)	Case No.
v.	)	Judge
NUANCE COMMUNICATIONS, INC., a Delaware for-profit corporation,	)	**COMPLAINT**
Defendant.	)	**(Jury Demand Endorsed Hereon)**

PRELIMINARY STATEMENT

1. This case arises from a destructive malware attack that caused substantial damage to plaintiff Heritage Valley Health System and its patients. The malware made its way into Heritage Valley's network through a trusted connection with a server owned and operated by defendant Nuance Communications, Inc.

2. The malware attack began in the Ukraine and initially entered into Nuance's network through its relationship with a software developer in that country. The malware spread through Nuance's network from India to Massachusetts and then back again before finally entering into Heritage Valley's systems in Pennsylvania.

3. Heritage Valley never should have been infected by the malware and never would have been infected by the malware were it not for Nuance's negligence. Nuance implemented a business strategy focused on global expansion without taking the precautions necessary to protect itself and its customers against foreseeable cybersecurity risks that were part and parcel of this international growth.

4. The result was that Nuance left itself defenseless against an eminently foreseeable malware attack and became a conduit for the attack to infect other entities. For Heritage Valley the attack ultimately caused the health system millions of dollars in damages, all of which could have been avoided had Nuance focused more of its attention on cybersecurity risk as opposed to international business growth.

5. As one of Nuance's largest shareholders subsequently wrote: "*Being hit by a malware is not an act of god; it's a result of poor security practices and governance oversight*." (Sept, 18, 2017 Lett., Amit Solomon to Robert J. Frankenberg, available at https://markets.businessinsider.com/news/stocks/neuberger-berman-delivers-letter-to-nuance-communications-board-of-directors-calls-for-immediate-ceo-and-board-changes-1011085836, last visited September 27, 2019) (emphasis in original).

PARTIES

6. Plaintiff Heritage Valley Health System, Inc. is a Pennsylvania non-profit corporation with its principal place of business in Beaver, Pennsylvania. Heritage Valley provides comprehensive health care for residents of Allegheny, Beaver, Butler and Lawrence counties in Pennsylvania, eastern Ohio, and the panhandle of West Virginia.

7. Defendant Nuance Communications, Inc. is a Delaware for-profit corporation with its principal place of business in Burlington, Massachusetts.

JURISDICTION AND VENUE

8. This Court has subject matter jurisdiction under 28 U.S.C. § 1332(a)(1), as the amount in controversy exceeds $75,000, exclusive of interest and costs, and the suit is between citizens of different states.

9. Venue is appropriate in this district under 28 U.S.C. §§ 1391(b)(1) and (2).

FACTUAL ALLEGATIONS

A. The June 27, 2017 NotPetya Malware Attack.

10. On June 27, 2017, a malware attack known as the NotPetya malware attack was directed at the Ukraine. It is believed the attack was initiated by a group of actors associated with the Russian government.

11. The malware was distributed through M.E.Doc, a Ukrainian tax-filing program. M.E.Doc is a popular service in the Ukraine, similar to TurboTax or Quicken in this country. When M.E.Doc installed a software update on user systems they downloaded the malware.

12. One month earlier, in May 2017, M.E.Doc was also responsible for the distribution of another malware known as XData. Ninety-five percent of victims of the XData malware were located in the Ukraine. *See generally* Lily Hay Newman, *Another Ransomware Nightmare Could Be Brewing In Ukraine*, Wired.com, 05.09.2017, available at https://www.wired.com/2017/05/another-ransomware-nightmare-brewing-ukraine/.

13. The Ukraine has often been the victim of cyberattacks. On December 23, 2015, for example, three Ukrainian energy companies were victimized by coordinated cyberattacks causing loss of power to approximately 225,000 households.

14. Much like the NotPetya malware, the KillDisk malware used in these attacks corrupted the Windows master boot record, rendering systems inoperable.

15. One year later, on December 17, 2016, cyberattackers infiltrated an electric transmission station north of Kiev, and were able to black out a portion of the Ukrainian capital. Researchers alternatively named the malware used in that attack as either Crash Override or Industroyer.

16. Thus, not only by June 2017 but also well before companies doing business in the Ukraine knew or should have known that the potential for cyberattacks directed at businesses in the Ukraine was very much a real threat.

B. Nuance Engages in a Business Strategy Focused on International Growth and Expansion.

17. Nuance proclaims itself to be a "leading provider of voice recognition and natural language understanding solutions." (Nuance Communications, Inc., Annual Report 1 (Form 10-K) (Nov. 22, 2016).) Nuance's "solutions and technologies are used in the healthcare, mobile, consumer, enterprise customer service, and imaging markets." (*Id.* at 18.)

18. Specific with respect to healthcare, Nuance offers several distinct product offerings, including medical documentation transcription services and Dragon Medical, which is a dictation software for use by physicians.

19. According to a June 2017 fact sheet, the company's healthcare solutions were deployed in 86 percent of all United States hospitals and more than 500,000 clinicians and 10,000 healthcare facilities worldwide used the company's clinical documentation solutions.

20. Throughout the course of its history Nuance has built itself through acquisition. Since 2006 alone the company has made more than fifty different corporate acquisitions. As one commentator stated in May 2013: "Over the last decade, Nuance Communications has been on a frenetic shopping spree." Robert Cyran, *Speech-tech firm's M&A machine could go in reverse*, Reuters Breakingviews (May 15, 2013), available at https://www.breakingviews.com/considered-view/speech-tech-firms-ma-machine-could-go-in-reverse/.

21. As a result of these and other acquisitions Nuance now has more than 150 corporate subsidiaries. More than half of these subsidiaries are headquartered internationally.

22. As Nuance boasts on its website: "With more than half of the organization residing outside of the US and a sales presence in more than 70 countries, Nuance can deliver solutions to numerous local markets and bring global perspective and capabilities to its solutions." Nuance.com, *Nuance office locations*, available at https://www.nuance.com/about-us/office-locations.html (last visited October 8, 2019).

23. Part of Nuance's global expansion has included doing business in the Ukraine. In September 2012 Nuance touted the fact that "Ukraine Joins the Dragon Mobile Apps Family!" *See* Sofie Bjorksten, *Ukraine Joins the Dragon Mobile Apps Family!*, Posted Sept. 26, 2012, previously available at https://whatsnext.nuance.com/connected-living/ukraine-joins-the-dragon-mobile-apps-family/.

24. The September 2012 press release, which is now no longer available on Nuance's website, stated that "[t]oday we launched our dynamic Dragon Dictation and Dragon Search apps for iOS in the Ukraine iTunes store! And they're already making waves . . . in fact, Dragon Dictation has already reached the #2 spot on the Ukraine App Store!!!!" *Id.*

25. Business Wire report's on the press release quoted Michael Thompson, executive vice president and general manager of Nuance Mobile, who stated: "We're very excited to continue expanding our global reach, bringing the power of Dragon to rapidly growing mobile markets like Ukraine." *See* Business Wire via the Motley Fool, *Nuance Dragon Dictation and Dragon Search Apps Now Available in Ukraine*, Sept.

26, 2012, available at https://www.businesswire.com/news/home/20120926005291/en/Nuance-Dragon-Dictation-Dragon-Search-Apps-Ukraine.

26. Part of Nuance's international growth has also included expanding its business operations into India, with nine separate subsidiaries incorporated in India and office locations in Karnataka, Haryana, Maharastra, and Uttar Pradesh.

27. In February 2017, just months before the NotPetya malware attack, Nuance acquired yet another company headquartered in India, named mCarbon. The acquisition closed in June 2017, just weeks before the NotPetya malware attack. *See* Danish Khan, *Nuance says mCarbon acquisition helps it expand service provider business globally*, European Times Telecom, June 1, 2017, available at https://telecom.economictimes.indiatimes.com/news/nuance-says-mcarbon-acquisition-helps-it-expand-service-provider-business-globally/58943817.

C. Nuance Falls Victim to the NotPetya Malware Attack Through a Trusted Development Partner in the Ukraine.

28. Around 7 a.m. on June 27, 2017, Satish Maripuri, the Executive Vice President and General Manager of Nuance's HealthCare Division, was driving to work when a colleague texted him that "an incident of abnormal nature" was gripping Nuance's computer networks.

29. Ten minutes later Maripuri received another text, stating that whatever was happening at the company was "a little more nefarious" than normal.

30. By the time he arrived at work Maripuri finally began to realize the actual severity of the situation: "We were down email, desktop IP phones. Networks were down," he later explained. *See* Ryan Black, *WannaCry, NotPetya, and Cyberwarfare's*

Threat to Healthcare, Healthcare Analytics News, June 11, 2018, available at https://www.idigitalhealth.com/news/wannacry-notpetya-and-cyberwarfares-threat-to-healthcare?p=3.

31. The problems for Nuance only worsened as the morning progressed. Ultimately, the NotPetya malware attack affected 14,800 Nuance servers of which 7,600 had to be replaced. The malware attack also affected 26,000 computer workstations of which 9,000 had to be replaced.

32. At some point on the morning of June 27, as the malware continued to spread through the company's systems, Nuance was forced to take its client-facing software solutions offline in a belated attempt to stop the malware from spreading to its customers. One client-facing software solution taken offline was iChart, which hosts an application called Dictaphone.

33. The next day Nuance finally admitted publicly that it had fallen victim to the NotPetya malware attack. In its press release Nuance downplayed the scope of the incident: "Nuance Communications, Inc. indicated that on Tuesday, June 27, portions of its network were affected by a global malware incident, which also affected many other companies and organizations worldwide." *See* June 28, 2017, Press Release, *Nuance Comments on Malware Incident*, available at https://www.nuance.com/about-us/newsroom/press-releases/nuance-comments-on-malware-incident.html.

D. For Nuance, Falling Victim to the NotPetya Malware was the Result of "Poor Security Practices and Governance Oversight."

34. Nuance became a victim of the NotPetya malware attack as a result of its own information security failings. The sheer number of Nuance's corporate acquisitions and the reach and pace of its global expansion combined to make meaningful

integration of acquired systems and meaningful segmentation of Nuance's growing global network difficult. Moreover, rather than expend the resources necessary to meet this growing cybersecurity risk, Nuance instead did not have or invest in the budget or management that would have been required to adequately address this issue.

35. To the contrary, Nuance's acquisition-driven business strategy riddled the company with debt. As of September 30, 2016, Nuance had more than $2.685 billion of debt outstanding. (Nuance Communications, Inc., Annual Report 14 (Form 10-K) (Nov. 22, 2016).) As Nuance disclosed in its filings: "***Our significant debt could adversely affect our financial health and prevent us from fulfilling our obligations under our credit facility and our convertible debentures.***" (*Id.* (emphasis in original).)

36. This combination of building the business through corporate acquisition, a drive toward global expansion, and significant corporate debt created a perfect storm of integration mismanagement which in turn created substantial cybersecurity risk. With each acquisition and international expansion Nuance exposed itself and its customers to increasing cybersecurity risk, all the while Nuance did not have the management or funding in place to sufficiently protect against these risks.

37. These business practices combined to make Nuance unprotected against an eminently foreseeable cyberattack. As one commentator subsequently wrote specifically with respect to the NotPetya malware attack: "Global companies with flat networks are super vulnerable to this." *See* Lesley Carhart @derbycon @hacks4pancakes, Replying to @ _noid_ @MalwareTechBlog, available at https://twitter.com/hacks4pancakes/status/879824553773498369.

38. Neuberger Berman, one of Nuance's largest shareholders since October 2012, made the same point in September 2017 correspondence. In this letter, Neuberger Berman noted the uniqueness of the NotPetya malware attack as pertained to Nuance. The letter stated: "To our knowledge [Nuance] is the largest technology company to have been materially impacted, with $240mm (or 9%) of on-demand contract value lost." (September 18, 2017 Letter from Amit Solomon to Robert J. Frankenberg, available at https://markets.businessinsider.com/news/stocks/neuberger-berman-delivers-letter-to-nuance-communications-board-of-directors-calls-for-immediate-ceo-and-board-changes-1011085836, last visited September 27, 2019).

39. Notably, from its position of unique insight into the company, Neuberger Berman wrote that the problems that caused Nuance to fall victim to the NotPetya malware attack were not at all external. As the shareholder told the company: "*Being hit by a malware is not an act of god; it's a result of poor security practices and governance oversight*." (*Id.*, emphasis in original.) The letter continued: "We are surprised no senior person at the company took responsibility for the incident, and believe responsibility begins at the top." (*Id.*)

E. Heritage Valley Health System Is Infected with the NotPetya Malware Through a Nuance Network Connection.

40. Ultimately, Nuance's business connections in the Ukraine and negligent information security practices became a conduit for the NotPetya malware to affect the United States healthcare system. *See, e.g.*, Paul Flahive, *Worldwide Ransomware Attack Affects Area Hospitals*, Texas Public Radio (June 28, 2017) ("Here in San Antonio the ransomware attack has disabled a leading provider of medical dictation

services from the company Nuance."), available at https://www.tpr.org/post/worldwide-ransomware-attack-affects-area-hospitals; Melanie Evans, *Cyberattack Forces West Virginia Hospital to Scrap Computers*, The Wall Street Journal (June 29, 2017), available at https://www.wsj.com/articles/cyberattack-forces-west-virginia-hospital-to-scrap-its-computer-systems-1498769889 (noting "[t]he cyberattack, known as Petya, froze the hospital's electronic medical record system early Tuesday").

41. This includes plaintiff Heritage Valley Health System. Specifically, at approximately 7:30 a.m. on Tuesday, June 27, 2017, Heritage Valley became a victim of the NotPetya malware attack.

42. As with Nuance the outbreak ultimately affected a majority of Heritage Valley's servers and workstations by encrypting the file system and files, making the operating systems unbootable and the files contained on the drives inaccessible.

43. A forensics analysis from two independent data sources showed that the malware entered Heritage Valley's computer network systems through a trusted virtual private network connection with Nuance.

44. The first source was security event logs recovered from a compromised host at Heritage Valley containing the user account credentials the malware used to spread. This is referred to as the flight path or flight recording of the malware.

45. The first compromised account found on the logs belonged to an unidentified domain with the user-service account dmytroD. Dmytro is a popular name in the Ukraine, and dmytroD's computer was either interconnected to Nuance or had an established trust relationship with Nuance.

46. The second credential belonged to the Nuance domain with the user-service account Prashant_tiwari. This account belongs to Prashant Tiwari, a Senior System Engineer at Nuance Communications, located in Pune, Maharashtra, India. *See* https://www.linkedin.com/in/prashant-tiwari-7b015028/.

47. The third and fourth credentials belonged to the HCE domain, the domain name of a Nuance business area called Nuance Healthcare. The third compromised account belonged to Pravallika Kothapalli, a Senior Project Manager at Nuance Communications in Burlington, Massachusetts. *See* https://www.linkedin.com/in/pravallika-kothapalli-96236212a/.

48. The fourth compromised user-service account from the Nuance Healthcare domain belonged to Sajid Siddiqui, a Principal Development Engineer at Nuance Communications, located in Pune, Maharashtra, India. *See* https://www.linkedin.com/in/sajid-siddiqui-7ab91a9/.

49. The fifth Nuance credential belonged to the iChart domain with the user-service account "ntservice." As pertains to Heritage Valley, this connection is related to an agreement the health system had entered into with Dictaphone Corporation in 2003. Under the agreement, Dictaphone was provided through a trusted point-to-point virtual private network connection known as iChart. Nuance subsequently acquired Dictaphone in 2006.

50. Finally, the sixth and seventh credentials identified were part of Heritage Valley's domain: TMCNET\eetapps and TMCNET\d5h5adm. The eetapps account was the first Heritage Valley account exploited by the NotPetya malware.

51. Thus, based on the malware's flightpath as shown above, a forensics analysis showed that the NotPetya malware entered into Heritage Valley's network

systems through Nuance, which in turn had been initially infected by the malware through a connection to a computer user located in the Ukraine.

52. This conclusion is consistent with Nuance's own public statements regarding the malware attack. In particular, Nuance has admitted that its systems became infected through a "trusted development partner" based in the Ukraine. *See* Ryan Black, *WannaCry, NotPetya, and Cyberwarfare's Threat to Healthcare*, Healthcare Analytics News, June 11, 2018, available at https://www.idigitalhealth.com/news/wannacry-notpetya-and-cyberwarfares-threat-to-healthcare?p=3.

53. A second forensics data source also supported the conclusion that Heritage Valley became infected with the NotPetya malware through Nuance. Specifically, Heritage Valley's firewall logs showed traffic indicative of the NotPetya malware originating from the virtual private network connection between Nuance and Heritage Valley during the first activity by the malware in Heritage Valley's network.

54. The firewall logs showed that at 7:23:44 AM EDT on June 27, 2017, the Nuance virtual private network connected to port 445 of a Heritage Valley server. This server was later determined to be the initial introduction of the malware into the Heritage Valley environment, through the installation and execution of PSEXESVC (PSExec service) on the server.

F. The NotPetya Attack Caused Immediate and Substantial Harm to Heritage Valley Health System.

55. The destruction the NotPetya malware caused to Heritage Valley Health System and its patients was immediate and substantial. The incident affected the entire health system including satellite and community locations. This included Heritage

Valley's Sewickley and Beaver hospitals, Heritage Valley Medical Group, Tri-State Obstetrics and Gynecology, and Heritage Valley Pediatrics.

56. The malware affected every aspect of the health system's ability to operate. Physicians and nurses were forced to re-draw pre-operative laboratory results because they could no longer access prior results. Bands had to be cut off and alarm systems rebooted each time an infant was discharged from the hospital. Laboratories and x-ray machines were down. Under these circumstances Heritage Valley physicians made critical decisions as to whether patients had to be diverted and if so to what location.

57. The fact that the quality of critical health care Heritage Valley provided to its patients did not suffer was the result of the extraordinary efforts of Heritage Valley physicians, nurses and administrative staff, who endured throughout the chaos of the malware attack to maintain continuity to patient care to the greatest extent possible.

58. At the same time, laboratory and diagnostic services at Heritage Valley medical neighborhoods and community locations were closed for days, and it was not until nearly a week later that all acute, ambulatory and ancillary care services were restored at all Heritage Valley locations.

59. Heritage Valley suffered millions of dollars in damages as a result of Nuance's negligence, including not only substantial business income loss but also the required repair and restoration of computer network systems, a significant amount of employee overtime and compensation, professional and third-party fees incurred in connection with responding to and remediating the incident, and intangible economic harm including the loss of goodwill.

60. Heritage Valley also continues to incur attorneys' fees and other expenses in responding to and remediating from the NotPetya malware incident, including relating to an ongoing regulatory investigation.

61. Heritage Valley brings this action to recover these damages, as attempts to even attempt to engage Nuance Communications in settlement negotiations have been unsuccessful.

COUNT I – NEGLIGENCE

62. Heritage Valley hereby incorporates the above-stated allegations by reference as if fully set forth herein.

63. Nuance engaged in affirmative conduct by implementing an acquisition-based business strategy focused predominantly on international growth. Through this affirmative conduct Nuance exposed the computer network systems of its customers and the customers of its subsidiaries to an unreasonable and foreseeable risk of harm in the form of the persistent threat of cyberattacks whether through malware or otherwise.

64. This affirmative conduct imposed a duty on Nuance to exercise reasonable care and to take proper precautions to ensure that Nuance's computer network systems were sufficiently protected against cyber intrusions, particularly when Nuance's networks maintained trusted connections with third-party entities, including plaintiff Heritage Valley.

65. Nuance breached this duty by failing to take proper precautions to protect its computer network systems against the threat of malicious intrusion. Nuance left its computer systems and the computer systems of its customers and the customers of its subsidiaries exposed to an unreasonable and foreseeable risk of harm in the form of malware and other cyber intrusions perpetrated on an international scale.

66. Nuance's breach of duty in failing to maintain adequate data security protections caused Heritage Valley to become a victim of the NotPetya malware attack. As shown above, the NotPetya malware entered Heritage Valley's network systems through a trusted network connection with Nuance.

67. Nuance's breach of duty caused substantial damages to Heritage Valley, including but not limited to lost business income related to the NotPetya malware attack; payments to third-parties in responding to and remediating from the malware attack; substantial costs to repair and remediate its computer network systems from the malware attack; employee overtime and compensation responding to and remediating from the malware attack; and other intangible economic harm, including the loss of goodwill.

COUNT II – BREACH OF IMPLIED IN FACT CONTRACT

(In the alternative to Count I)

68. Apart from the allegations in Count I, Heritage Valley hereby incorporates the above-stated allegations by reference as if fully set forth herein.

69. Heritage Valley entered into an agreement with Dictaphone Corporation in 2003. Under this agreement Dictaphone was provided to Heritage Valley through a trusted point-to-point virtual private network connection known as iChart.

70. Nuance subsequently acquired Dictaphone in 2006 and maintained the corporation as a wholly-owned subsidiary.

71. Heritage Valley continued to use the Dictaphone product having paid more than $3.1 million for its use of Dictaphone since the inception of the relationship.

72. In continuing to accept the benefits of this agreement and continuing to maintain this trusted connection Nuance impliedly contracted to take reasonable security measures to protect its computer network systems against cyber intrusion.

73. Nuance breached this implied contract by failing to adequately protect its computer network system against potential cyberattack and by failing to protect its customers and the customers of its subsidiaries from becoming the collateral victim of a successful intrusion into one portion of Nuance's computer network systems.

74. As a result of Nuance's breach of implied contract Heritage Valley became a victim of the NotPetya malware attack and has suffered substantial damages, including but not limited to lost business income; payments to third-parties in responding to and remediating from the incident; substantial costs to repair and remediate its computer network systems from the incident; employee overtime and compensation responding to and remediating from the incident; and other intangible economic harm.

COUNT III – UNJUST ENRICHMENT

(In the alternative to Count Two)

75. Apart from the allegations in Count II, Heritage Valley hereby incorporates the above-stated allegations by reference as if fully set forth herein.

76. Heritage Valley conferred a benefit on Nuance in the form of payments made to its wholly-owned subsidiaries, including Dictaphone Corporation.

77. Nuance appreciated these benefits which were commingled with its own revenues and the revenues of Nuance's other subsidiaries for Nuance's own financial benefit.

78. Nuance failed to maintain adequate data security practices to protect Heritage Valley and other customers of its subsidiaries from becoming the indirect victim of a cyberattack, instead choosing to implement a business strategy focused on rapid international growth.

79. Under these circumstances it would be unjust for Nuance to retain the benefit of payments Heritage Valley has made to Nuance and its subsidiaries.

PRAYER FOR RELIEF

Based on the above-stated allegations, Heritage Valley prays for judgment in its favor and against Nuance as follows:

A. Compensatory damages in an amount to be proven at trial;

B. Punitive damages against Nuance to the extent recoverable by Pennsylvania law;

C. All attorneys' fees incurred in connection with this litigation;

D. A declaration that Nuance is responsible for reimbursing Heritage Valley for any future costs and/or penalties Heritage Valley suffers as a result of the NotPetya malware incident;

E. Interest, costs, and all other such relief as this Court may deem appropriate in the exercise of its discretion.

JURY DEMAND

Heritage Valley hereby demands a trial by jury as to all issues so triable.

Dated: November 27, 2019

Respectfully submitted,

/s/ Julian D. Perlman

Julian D. Perlman
BAKER & HOSTETLER LLP
2929 Arch Street
Cira Centre, 12th Floor
Philadelphia, PA 19104-2891
Tel: (215) 568-3100
jperlman@bakerlaw.com

David A. Carney (*pro hac vice forthcoming*)
BAKER & HOSTETLER LLP
127 Public Square, Suite 2000
Cleveland, OH 44114-1214
Tel: (216) 621-0200
dcarney@bakerlaw.com

Attorneys for Heritage Valley Health System